PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Rolf E. Carlson	Group Art Unit 2136
Appl. No.:	09/698,507	
Filed:	October 26, 2000	
For:	CRYPTOGRAPHY AND CERTIFICATE AUTHORITIES IN GAMING MACHINES	
Examiner:	Brandon S. Hoffman	

DECLARATION UNDER 37 C.F.R. § 1.131

1. I am currently a shareholder in Dorr, Carson, Sloan, Birney & Kramer, 3010 East Sixth Avenue, Denver, Colorado 80206; (303) 333-3010.

2. From at least March, 1999 until November, 1999, I worked as a full-time patent attorney in the law firm of Dorr, Carson, Sloan & Birney, P.C. During this time, John Thompson, Esq. was an Associate in our law firm's employ.

3. From at least April 8, 1999 until September 30, 1999, I supervised the preparation by Mr. Thompson of, on information and belief, several drafts for provisional application no. 60/161,591 (the '591 provisional application). Appendix A includes a copy of time sheets documenting Mr. Thompson's approximately 170 hours of work on the '591 provisional application from April through September of 1999. Our firm's Docket Number for the preparation of the '591 provisional application is identified as either "Mikohn/246" or "1482/426" in Appendix A. The initials "JFT" refer to Mr. Thompson. Unrelated billing has been redacted out. Mr. Thompson worked on many other matters during that time frame.

4. On October 13, 1999, I informed the inventor, Mr. Carlson, that Mr. Thompson was leaving the firm and I provided a revised draft of the '591 provisional application (Appendix B) to Mr. Carlson that incorporated his changes in conversations, on information and belief, given to Mr. Thompson.

5. On October 23, 1999, Mr. Carlson requested that I file the '591 provisional application before transferring the case to a new patent attorney, Peter Lippman, Esq.

6. On October 26, 1999, I filed the '591 provisional application.

7. On November 11, 1999, the '591 provisional application file was transferred to Peter Lippman, Esq.

Penalty of Perjury Statement

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent resulting there from.

Dated: 7/6/05

By: Robert C Dorr

Robert C. Dorr, Esq.
DORR, CARSON, SLOAN, BIRNEY
& KRAMER, P.C.
Reg. No. 27,782
3010 East 6th Avenue
Denver, Colorado 80206
(303) 333-3010

F:\rcd\MIKOHN\Carlson\37 CFR 1 131 Declaration.doc

P.O. BOX 262
PETERSBURG, PA 16669

(800) 544-4748 • (814) 667-2580

1.A — Attend/A ence
2.C — Confer/C
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel
11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time hours	Time tenths
				T-		

2/15

4/8/99	Mi Kohn / 246	1487 / sub	Review Information from Inventor regarding Certificate of Authorities	JFT	3	9

TIME RECORD (FORM S-3)

ROSEMONT FORMS, INC.
P.O. BOX 262
PETERSBURG, PA 16669

(800) 544-4748 • (814) 667-2580

CLIENT TIME
1.A — Attend/Confer/Conference
2.C — Confer/Conference
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel

NON-CLIENT TIME
11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

DECIMAL CONVERSION
6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time hours	Time tenths
4/9/99	MiKohn / 246	1482/246	Conference with Rolf Carlson	JFT	0	6
		1482/246	- patentability analysis			
4/19/99	MiKohn / 246	1482/246	Continue to draft Patent Application	JFT	5	2

3/15

4/20/99	MiKohn / 246	1482/246	Continue to draft patent application	JFT	5	8
4/21/99	MiKohn / 246	1482/	Continue to draft Patent	JFT	3	8

ROSEMONT FORMS, INC.
P.O. BOX 262
PETERSBURG, PA 16669

(800) 544-4748 • (814) 667-2580

TIME RECORD (FORM S-3)

CLIENT TIME
1.A — Attend/ r
2.C — Confer, rence
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel

NON-CLIENT TIME
11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

DECIMAL CONVERSION
6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time	
4/22/99	MiKohn / 246	1482/ /246	Continue to drgt Patent Application	JFT	3	7
4/23/99	MiKohn / 246	1482/ /246	Continue to prepare Patent Application	JFT	4	7
4/26/99	MiKohn / 246	1482/ /246	Continue to prepare Patent Application	JFT	5	7
4/27/99	MiKohn / 246	1482/ /246	Continue to drgt Application	JFT	3	7
4/28/99	MiKohn / 246	1482/ /246	Continue to prepare	JFT	4	2

4/15

ROSEMONT FORMS, INC.
P.O. BOX 262
PETERSBURG, PA 16669
COPYRIGHT © 1996
(800) 544-4748 • (814) 667-2580

CLIENT TIME

1.A — Attend/[illegible]r
2.C — Confer[illegible]rence
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel

NON-CLIENT TIME

11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

DECIMAL CONVERSION

6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time hours	Time tenths
4/29/99	MiKohn / 246	1482/	Continue to draft	JFT	6	8
		/246	Patent Application			
4/30/99	MiKohn / 246	1482/	Continue to draft	JFT	6	1
		/246	Patent Application			

5/15

TIME RECORD (FORM S-3)

ROSEMONT FORMS, INC.
P.O. BOX 262
PETERSBURG, PA 16669
COPYRIGHT © 1996
(800) 544-4748 • (814) 667-2580

CLIENT TIME
1.A — Attend/Appear
2.C — Confer/Conference
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel

NON-CLIENT TIME
11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

DECIMAL CONVERSION
6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time hours	Time tenths
5/3/99	MiKohn/246	1482/246	Prepare Patent Application; Draft [redacted] Claims	JFT	5	6
5/4/99	MiKohn/246	1482/246	Continue to prepare Patent Application; continue to prepare claims	JFT	6	2
5/5/99	MiKohn/246	1482/246	Continue to prepare patent application; draft claims	JFT	4	1
5/6/99	MiKohn/246	1482/246	Prepare application, begin to draft background.	JFT	4	5
		100	Review inventor's comments			
5/10/99	MiKohn/246	1482/246	Continue to draft background	JFT	6	4
5/12/99	MiKohn/246	1482/246	Begin to prepare disclosure	JFT	6	2
5/13/99	MiKohn/246	1482/246	Continue to prepare disclosure; draft detailed description	JFT	2	6

6/15

APPENDIX A

TIME RECORD (FORM S-3)

ROSEMONT FORMS, INC.
P.O. BOX 262
PETERSBURG, PA 16669

(800) 544-4748 • (814) 667-2580

CLIENT TIME

1.A — Attend/Appear
2.C — Confer/Conference
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel

NON-CLIENT TIME

11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

DECIMAL CONVERSION

6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time
		188	discussion ...		
5/21/99	MIKohn/246	1482/	Continue to prepare	JFT	1 5
		/246	detailed description		
5/25/99	MIKohn/246	1482/	Continue to prepare	JFT	3 6
		/246	Application		
					7/15
5/26/99	MIKohn/246	1482/	Continue to prepare	JFT	3 9
		/246			

TIME RECORD (FORM S-3)

ROSEMONT FORMS, INC.
P.O. BOX 262
PETERSBURG, PA 16669

(800) 544-4748 • (814) 667-2580

CLIENT TIME

1.A — Attend/Appear
2.C — Confer/Conference
3.D — Draft
4.I — Instruct
5.J — Investigate
6.L — Dictate/Letter
7.R — Research
8.S — Study/Review
9.T — Telephone
10.V — Travel

NON-CLIENT TIME

11.E — Education/Reading
12.M — Office Management
13.X — Bar/Community Activities
14.P — Personal
15.Y — Vacation

DECIMAL CONVERSION

6 minutes=.1 hour
12 minutes=.2 hour
18 minutes=.3 hour
24 minutes=.4 hour
30 minutes=.5 hour
36 minutes=.6 hour
42 minutes=.7 hour
48 minutes=.8 hour
54 minutes=.9 hour
60 minutes=1.0 hour

Date	Client / Matter	File No. Non-Cl. Time	Work Done	Lawyer	Time hours	Time tenths
6/22/99	McKohn / 246	1482/246	Begin to review Inventor's Comments	JFT	4	1
6/23/99	McKohn / 246	1482/246	Review Prior Art	JFT	7	1
6/24/99	McKon / 246		Continue to review prior art	JFT	6	8
6/25/99	McKohn / 246	1482/246	Continue to review Inventor's Comments	JFT	6	2
6/28/99	McKohn / 246	1482/246	Draft Claims	JFT	7	5
6/29/99	McKohn / 246	1482/246	Continue to Draft Claims	JFT	7	2
6/30/99	McKohn / 246	1482/246	Continue to Draft Claims	JFT	6	7
				JFT	8	5

8/15

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	TIME		
7/6/99	1482/246 MiKohn	Review claims; draft additional claims	3	8	JFT
7/8/99	1482/246 MiKohn	Continue to draft claims	5	2	JFT
7/9/99	1482/246 MiKohn	Continue to draft claims; begin to prepare figures	6	7	JFT

Date Entered _____ By: _____

9/15

MilKohn Time JFT

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	TIME		
7/12	1482/246 MilKohn	Continue to drgt patent application; Finalize claims, and drawings	5	5	JFT
7/13	1482/246 MilKohn	Draft Background and Summary and Abstract of patent application	5	9	JFT
7/14	1482/246 MilKohn	Drgt Detailed Description of Patent Application	5	7	JFT
7/15	1482/246 MilKohn	Continue to Drgt Detailed Description	7	0	JFT
					JFT
7/16	1482/246 MilKohn	Continue to drgt Detailed Description	5	3	JFT

5/01

Date Entered _____ By: _____

MiKohn Time JFT

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	TIME		
7/19/99	MiKohn 1482/246	finalize draft of application; Continue to revise draft	4	0	JFT
7/20/99	MiKohn 1482/246	Continue to revise draft of application	4	5	JFT
					FT
					FT
					FT
7/21/99	MiKohn 1482/246	Continue to revise draft of invention disclosure	3	3	JFT
7/22/99	MiKohn 1482/246	Continue to revise draft of Patent application	1	7	JFT
					JFT
					FT

SI/15

MIKOHN BILLING FORM
JOHN F. THOMPSON
$140/HOUR

8/16/99 to 8/20/99

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	COST	TIME	
					2
					2
					8
8/19/1999	1482/246	Review Application relating to Certificate Authorities		2	2
8/1					7
8/2					1
8/20/1999	1482/246	Continue to Review Application; Begin to Finalize draft for Inventor's Review		1	2

5/21

MIKOHN BILLING FORM
JOHN F. THOMPSON
$140/HOUR

August 23, 1999 to August 27, 1999

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	COST	TIME	
				1	0
8/23	1482/246	Continue to Review Patent Application		3	3
8/24	1482/246	Continue to Review and Finalize Patent Application		4	1
8/25					
8/2					3
8/2					6

13/15

MIKOHN BILLING FORM
JOHN F. THOMPSON
$140/HOUR

Sept. 27, 1999 to October 1, 1999

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	COST	TIME	
$				.	2
9/28/99	MiKohn 1482/246	Telephone conference with Rolf Carlson; Draft Disclosure of Application		2	3
8/29/99	MiKohn 1482/246	Telephone Conference with Rolf Carlson; Continue to Draft disclosure		2	6
!				)	4
9/30/99	MiKohn 1482/246	Draft Memo relating to Patent application		0	4

17/15

MIKOHN BILLING FORM
JOHN F. THOMPSON
$140/HOUR

Sept. 20, 1999 to Sept. 24, 1999

DATE	CLIENT ACCOUNT	SERVICES PERFORMED	COST	TIME	
9/20/99	Mikohn 1482/246	Telephone conference with Rolf Carlson; begin to draft claims and specification		2	3
9				?	2
9/22/99	1505/5(a)	Continue to draft response		1	3
9/23/99	Mikohn 1482/246	Telephone conference; continue to draft claims and specification.		2	8
9/23					3
9/2					1

51/51

CRYPTOGRAPHY AND CERTIFICATE AUTHORITIES IN GAMING MACHINES

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The present invention relates to an apparatus and method for encrypting communications on a network bus in a gaming system, and more particularly, to an apparatus and method where a certificate authority server manages keys used to secure communications on a network bus in a gaming system.

2. Statement of the Problem.

Conventional gaming machines include a processor, a rules library, a random number generator and an interactive display. In the casino, these conventional gaming devices are, typically, stand-alone type machines. Increasingly, the gaming machines in a casino are networked via a network bus to a gaming server. This networking is desired because it allows the casino to monitor wagering and other activities performed at each of the networked gaming machines. Since the monitoring of wagering and other activities performed at each of the networked gaming machines can include financial information, the casino desires that the communications over the network bus be secure.

In considering secure gaming communications, there are several important goals that should be addressed. The network bus should ensure privacy. Privacy, also termed confidentiality, is the

condition where the information is kept secret from all but those authorized to access the information. In the gaming environment, privacy can apply to the transmitted information as well as the identity of a player of the gaming machines.

In addition, information transmitted over the network bus should be authenticated. Authentication ensures that the content, integrity of the transmitted information, origin of the transmitted information, date of transmission, time of transmission and other attributes of the transmitted information have not been tampered with during transmission.

Additionally, entities transmitting information over the network bus should not be capable of repudiating the transmission. Cryptographic services that facilitate non-repudiation prevent a player and/or a casino from denying a previous action or commitment. The casino desires non-repudiation, especially, to enforce payment by a player that has wagered and lost. Conversely, the player desires non-repudiation to enforce payment by the casino when the player wins.

As a result of networking of the gaming machines, the ubiquity of the Internet, greater connectivity between networks, and the support for electronic commerce both inside and outside the casino, the casino desires secure communications over the network bus that provides privacy, authentication and non-repudiation. Therefore, a need exists to provide these services to support secure communication over the network bus between the gaming server and the gaming machines in a casino.

In addition, the casino may decide or desire to connect the gaming server and, hence, the network bus and all networked gaming machines, to an outside network. Networking the casino to an outside network may be advantageous for a gaming entity that owns several

casinos in different locations. For example, the connection of each casino to a centralized computer would provide centralized accounting of financial information for all the casinos operated by the gaming entity.

If casinos are connected to outside networks, however, it is critical that communications originating within the casino (including gaming machines and the gaming server) remain secured against misuse or tampering by an unauthorized party after the information exits the physical protection of the casino. This desire for secured communications becomes particularly important when financial information is transmitted by the casino over the outside network. Consequently, a need exists for a secure communication link between the gaming server in a casino and an outside network.

In addition, the connection between gaming machines requires various transmission and/or data protocols. These protocols are typically created as standards in the industry. However, a game manufacturer would like to control the connection between the gaming machines such that only authorized personnel can connect the gaming machines. Therefore, a need exists for a technique to control the connection between the gaming machines such that only authorized personnel can properly connect the gaming machines.

Additionally, some casino players may prefer playing a specific gaming machine. However, the player may be in a remote location and unable to travel to the casino to play. In such instances, the casino can connect a gaming machine to an outside network so that the player can connect to the outside network via a remote computer and play, even though absent from the casino. In such instances, a need exits for a secure network that provides privacy, authentication and non-repudiation so that the player can play and both the player

and casino can be confident in the knowledge that the transmitted information is secure and that the rules of the game will be upheld with integrity.

3. **Solution to the Problem**.

The present invention provides a method and apparatus that allows secure communication in a casino between networked gaming machines and a gaming server. With the present invention, privacy is ensured; communication is authenticated; and messages cannot be repudiated.

Additionally, the present invention discloses a method and apparatus that provides secure communications between the casino and an outside network. The present invention is especially advantageous if the gaming entity manages machines at multiple casinos in different locations and the gaming entity requires quick, yet secure retrieval of information over the outside network.

In addition, the present invention provides a method and apparatus for secure communications between each gaming machine. In this regard, this secure communication allows for the connection between the gaming machines to be controlled by the game manufacturer such that the gaming machines cannot be connected unless the cryptographic technique used to secure the communications between the gaming machines is known.

Lastly, the present invention provides secure communications between the casino and a remote player over an external network. The present invention is especially critical in ensuring that transmitted information between player and casino is kept confidential and

indecipherable by unauthorized individuals intercepting the transmitted information.

SUMMARY OF THE INVENTION

The present invention provides a casino gaming system having a plurality of gaming machines. In the Asymmetric case, Aa gaming server is provided that includes a plurality of long term keys from which it may generate ~~session~~ keys used to communicate between gaming machines and also between the gaming machines and server. Prior to use, Eeach of the ~~session~~ keys ~~has a~~ is time stamped. ~~that indicates a period of time for which each of the session keys is used.~~ The gaming server also includes a random number generator that is used to facilitate ~~capable of generating~~ generation of the ~~session~~ keys. The gaming server also includes an encryption algorithm.

A network bus is provided that interconnects the gaming machines and the gaming server. The network bus provides a communication link for transmitting information between the gaming machines and the gaming server. The gaming server uses the encryption algorithm to encrypt the ~~session~~ keys and transmits the encrypted ~~session~~ keys over the network bus to the gaming machine. Likewise, the gaming machines use the ~~session~~ keys to encrypt information and transmit the encrypted information over the network bus. In one aspect, the encrypted information is transmitted via the network bus to another of the gaming machines. In another aspect, the encrypted information is transmitted via the network bus to the gaming server.

In another embodiment, the casino gaming system includes an outside network that is connected to the gaming server. A remote computer is also provided that connects to the outside network so that the encrypted information is transmitted over the network bus and the

outside network to the remote computer. In one aspect, the outside network comprises the Internet.

In another embodiment of the present invention, the gaming server is a certificate authority server having a memory. In this aspect, the ~~session~~ keys are public keys of asymmetric key pairs which are stored in the memory at the certificate authority server. In addition, the certificate authority server may generate and transmits the public keys over the network bus to the gaming machines, or the public/private key pairs may be generated by a third party and delivered to the certificate authority for authentication.

In a further embodiment of the present invention, a plurality of access switches are each connected to a different one of the gaming machines. The network bus is connected to the gaming server and each of the access switches. In this embodiment, an outside network is connected to the gaming server and the access switches provide a communication link between specific gaming machines and a remote computer over the outside network when the specific gaming machine is idle, so as to enable a remote player of the remote computer to play the specific gaming machine.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates one embodiment of the casino gaming system of the present invention;

Fig. 2. is a flow chart showing a method for communicating information using a casino gaming system of the present invention;

Fig. 3 illustrates an embodiment of the casino gaming system of the present invention using a certificate authority server;

Fig. 4 illustrates another embodiment of the casino gaming system of the present invention; and

Fig. 5 is another embodiment of a method for communicating using the casino gaming system of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

I. Overview

In Fig. 1, a highly simplified gaming system 100 includes a gaming server 110 that is connected to a plurality of gaming machines 120-124 via network bus 130. The gaming server 110 can comprise, for example, a micro-computer or a network server. The connection of the gaming server 110 to network bus 130 can comprise, for example, a hard-wired communication link connection or a wireless communication link connection. The network bus 130 also connects to the plurality of gaming machines 120-124 that are located in a casino. In one embodiment, the gaming machines 120-124 can comprise conventional stand-alone gaming machines that are networked to the gaming server 110 via the network bus 130. The gaming machines 120-124 can also allow play of various conventional casino games such as, but not limited to, slots, poker, blackjack, etc.

In one embodiment, the casino gaming system 100 can also includes an outside network 140, such as, for example, the Internet, a Local Access Network (LAN) or a Wide Area Network (WAN). At least one remote computer 150 is connected to the outside network 140. In one embodiment, the connection of the remote computer 150 to the outside network 140 also enables the remote computer 150 to connect to the gaming server 110, and hence, the network bus 130 and the gaming machines 120-124. In this embodiment, a remote player of the remote computer 150 can play a specific one of the gaming machines 120-124 on the network bus 130 through the connection to the outside network 140. As such, a remote player can

play a specific one of the gaming machines 120-124 via an outside network 140 without having to be physically in the casino.

The connection between the network bus 130 and the gaming server 110 is conventionally known in the art, and the connection can include other equipment (not shown) such as, for example a router. The connection between the gaming server 110 and the outside network 140 is also know in the art, and the connection can include various security features, such as, for example, a firewall. The connection between the remote computer 150 and the outside network 140 can include, for example, a hardwire connection, a wireless connection or a modem connection. It should be appreciated that the present invention is not limited to the manner in which the components are connected, since such connection of the components is known in the art.

In the gaming system 100 of the present invention, information that is transmitted over the network bus 130 and the outside network 140 must be secure, especially with regard to financial information, such as, for example, player credit card information, player wagering information and casino pay-out information. To ensure a secure transmission of information over the network bus 130 and the outside network 140, the information is encrypted using various cryptography techniques. ~~Session~~ Kkey cryptography and certificate authority techniques are described below with regard to secure encrypted information transmission in a casino gaming system 100.

II. ~~Session~~ Key Cryptography

A. Casino Gaming System using ~~Session~~ Keys

In Fig. 1, the casino gaming system 100 includes a network 130 that interconnects gaming machines 120-124 and gaming server

110. The network bus 130 provides a communication link for transmitting information between the gaming machines 120-124, themselves, and between the gaming machines 120-124 and the gaming server 110. It should be noted that the computational capabilities of the gaming server 110 should generally exceed those of the gaming machines 120-124, at least with respect to cryptographic operations. In this regard, many computer systems have architecture and/or use compilers that physically limit the bit length of an integer, such as, for example, 32 bit length. However, key cryptography requires the use of very large integers having a bit length such as, for example, 64 or 256 bits. To enable these computer systems to arithmetically manipulate these integers, cryptographic primitives are required. Cryptographic primitives include algorithms that process large integers during various arithmetic processes. It should also be noted that these cryptographic primitives can be any algorithm that allows processing of large bit length integers by these bit-limited computer systems.

However, these primitives should be able to support Rivest, Shamir, and Adleman (RSA), El Gamal and other known key cryptographic algorithms. It should also be appreciated that the present invention is not limited by the algorithms and/or cryptography used to manipulate these large bit length integers, and the present invention encompasses any technique known and practiced in the art.

The gaming server 110 also includes ~~session~~ keys 160. For example, the ~~session~~ keys 160 can comprise, as will be described later, symmetric ~~session~~ keys, ~~or~~ asymmetric ~~session~~ keys or session keys. The ~~session~~ keys 160 include a time stamp 165 that indicates a period of time for which each of the ~~session~~ keys 160 is valid. The

time stamp 165 also ensures that the ~~session~~ keys 160 are changed on a periodic basis to provide a more secure communication link.

The gaming server 110 also includes a random number generator 170 that is used by the gaming server 110 to generate the ~~session~~ keys 160. The random number generator 170 can comprise a pseudo-random number generator and/or a random number generator that has been approved by a governmental regulation agency. The generation of the ~~session~~ keys 160 by using the random number generator 170 is known in the art and the present invention should not be limited to any one technique for generating the ~~session~~ keys160. It should also be appreciated that in another embodiment the random number generator 170 is optional. In this embodiment, the gaming server 110 receives the ~~session~~ keys 160 from another device (not shown) connected to the network bus 130.

It should also be appreciated that the gaming server 110 can also include an encryption algorithm 180. The gaming server 110 uses the encryption algorithm 180 to encrypt information or data before it is transmitted over the network bus 130. The encrypted information is decrypted before it is used. The encryption algorithm 180 can comprise, for example, a symmetric key or one of an asymmetric key pair as will be explained herein below.

In one embodiment, the gaming server 110 transmits at least one of the ~~session~~ keys 160 over the network bus 130 to a gaming machine 120. It should be appreciated that the gaming server 110 can transmit one of the ~~session~~ keys 160 to any one of the gaming machines 120-124 on the network bus 130. However, for ease of description, this discussion will focus on transmission to gaming machine 120.

In this embodiment, the gaming machine 120 uses the ~~session~~ keys 160 to encrypt information, such as, player credit card information, player identification information, wagering information and casino payout information. This encrypted information is transmitted over the network bus 130.

In one aspect, the encrypted information is transmitted over the network bus 130 to the gaming server 110. In another aspect, the encrypted information is transmitted over the network bus 130 from gaming machine 120 to another of the gaming machines 122-124. At the other gaming machine 122-124, the encrypted information is decrypted based on the type of ~~session~~ key 160 used as will be described herein below.

In another embodiment, the casino gaming system 100 includes an outside network 140 that is connected to the gaming server 110. The outside network 140 is connected to a remote computer 150. The outside network 140 comprises, for example, the Internet, a local access network (LAN) or a wide area network (WAN). In this embodiment, the gaming server 110 includes various known security mechanisms (not shown), such as, a firewall.

In this embodiment, the gaming server 110 transmits the ~~session~~ key 160 to gaming machine 120. The gaming machine 120 encrypts information using the ~~session~~ key 160 and transmits the encrypted information over the network bus 130. In one aspect of the present invention, the encrypted information is transmitted to the gaming server 110. In another aspect of the present invention, the encrypted information is transmitted by the gaming machine 120 to another of the gaming machines 122-124 on the network bus 130. In even another aspect, the encrypted information is transmitted to the outside network 140 and, ultimately, to the remote computer 150.

Once the encrypted information has been received, it is decrypted based on the type of ~~session~~ key 160 used, as will be described herein below. The information is then processed as required.

1. Symmetric ~~Session~~ Keys

As explained above, the ~~session~~ keys 160, in one embodiment, comprise symmetric ~~session~~ keys. Symmetric ~~session~~ keys, also termed private keys, use a unique key to encrypt and exchange information between two parties. In this embodiment, gaming machine 120 (the sender) and gaming server 110 (the recipient) share a symmetric ~~session~~ key k which is secret. In this embodiment, the gaming machine 120 encrypts information m before transmitting it over the network bus 130 to the gaming server 110. If symmetric encryption algorithm E and symmetric ~~session~~ key k are used, the encryption of m by E under k is denoted $c = E_k(m)$ where c represents the cipher-text associated with information m. Therefore, gaming machine 120 transmits cipher-text c over the network bus 130 to the gaming server 110. At the gaming server 110, the cipher-text c is decrypted using the symmetric ~~session~~ key k. The gaming server 110 applies the decryption algorithm $m = E_k^{-1}(c)$ to decrypt cipher-text c and obtain information m.

In addition, the symmetric key k can also be a session key. A session key is used for a specific exchange of a message m between two parties, such as, two gaming machines 120 and 122 or between a gaming machine 120 and the gaming server 110. In this embodiment, gaming machine 120 desires to communicate with gaming machine 122. The gaming server 110 contains a symmetric encryption function, E, that allows the encryption of a *session key*, k,

that will be sent by the gaming server 110 in an encrypted format to gaming machines 120 and 122. In this embodiment, $E_{k_i}(m)$ represents the encryption of message m under encryption algorithm E using key k_i, and $E_{k_i}^{-1}(m)$ represents the decryption of message m under encryption algorithm E using key k_i. In order to allow the communication between gaming machines 120 and 122, the gaming server 110 generates a new unique session key k, and the gaming server 110 sends $E_{k1}(k)$ to gaming machine 120 and $E_{k2}(k)$ to gaming machine 122. The gaming machines 120 and 122 each can recover the session key k by forming $k = E_{k1}^{-1}(E_{k_2}(k)) = E_{k21}^{-1}(E_{k_2}(k))$. Using the session key k, gaming machine 120 can communicate message m to gaming machine 122 by sending $E_k(m)$ to gaming machine 122. gaming machine 122 can form $m = E_k^{-1}(E_k(m))$ to recover the message. It should be appreciated that this technique can be used with communciations between any device connected to the network bus 130 and should not be limited to communications between only gaming machines 120 and 122. In addition, in one embodiment, the gaming server 130 generates the session key k using the long term asymmetric key 160 as a seed to random number generator 170. In another embodiment, the gaming server can use any one way function that is non-invertable to generate the session key k. However, it should be appreciated that the present invention can use any technique known in the art to generate the session key k, and the present invention should not be limited to only those disclosed.

It should be noted that the cipher-text c is described as being transmitted only from the gaming machine 120 to the gaming server

110. However, it should be understood that the cipher-text c can be transmitted from the casino gaming server 110 to the gaming machine 120 using the same symmetric ~~session~~ key 160. Moreover, it should be appreciated that cipher-text c can be transmitted from any one of the gaming machines 120-124 to the gaming server 110 or vise versa using the symmetric ~~session~~ key 160. In addition, the cipher-text c can be transmitted from the gaming machines 120-124 or the gaming server 110 to the outside network 140 and the remote computer 150 (or vise versa) using the symmetric ~~session~~ key 160 as described above. It should further be appreciated that the encryption algorithm 180 used by the gaming server 110 to encrypt and transmit the ~~session~~ keys 160 to the gaming machines 120-124 can comprise a symmetric ~~session~~ key 160, and the ~~session~~ key 160 can be encrypted and/or decrypted as described above with reference to information m. In a preferred embodiment, the symmetric ~~session~~ key 160 uses the Data Encryption Standard (DES) or one of the variants of DES such as triple-DES, DES-X or Advanced Encryption Standard (AES).

2. ~~Asymmetric Session Keys~~

As mentioned above, the ~~session~~ keys 160 can comprise asymmetric ~~session~~ keys. Asymmetric ~~session~~ keys, also termed public keys, use two different keys in a transaction. The asymmetric ~~session~~ key pair consists of a public and a private key. The public key is made available to all devices on the network bus 130 and the outside network 140 while the private key is kept secret. The essential feature of a public key cryptographic system is that knowledge of a public key does not provide computational information about the private key.

In this embodiment, the asymmetric ~~session~~ key pair 160 is represented by (u,r) where u represents the public key and r represents the private key. The gaming machine 120 acquires the public key u of the gaming server 110 from the gaming server 110 or another device (not shown) connected to the network bus 130 or the outside network 140. The gaming machine 120 encrypts information m using public key algorithm E_u. As a result, the cipher-text c is $c = E_u(m)$. The cipher-text c is transmitted to the gaming server 110 over the network bus 130. The private key algorithm E_r^{-1} is used by the gaming server 110 to decrypt the cipher-text c and therefore obtain the information $m = E_r^{-1}(E_u(m))$. In this embodiment, it should be appreciated that each of the gaming machines 120-124, the gaming server 110 and the remote computer 150 have a unique asymmetric ~~session~~ key pair (u,r). The public key u is provided to the sending party and only the private key r can decrypt information encrypted by the public key u. It should also be appreciated that the asymmetric ~~session~~ key technique can be used by any device connected to the network bus 130 or the outside network 140 so long as the appropriate public key u is used to encrypt the information m and the cipher-text c is sent to the device having the corresponding private key r.

In addition, it should also be appreciated that the encryption algorithm 180 can comprise the public key u of the asymmetric key pair (u,r). The gaming server 110 encrypts the ~~session~~ key 160 using the public key u and transmits the encrypted ~~session~~ key 160 to the appropriate gaming machine 120-124 or remote computer 150 having the corresponding private key r. In a preferred embodiment of the present invention, the asymmetric ~~session~~ keys 160 comprise

Rivest, Shamir, and Adleman (RSA) and El Gamal asymmetric algorithms.

3. Digital Signatures

In another embodiment, the ~~session~~ keys 160 can comprise a digital signature. A digital signature can be constructed by reversing the asymmetric ~~session~~ key technique described above. In this embodiment, the gaming machine 120 uses the private key algorithm E_r^{-1} to encrypt the information m where the cipher-text is $c = E_r^{-1}(m)$. The cipher-text c is transmitted to the gaming server 110 where the cipher-text c is decrypted to obtain information m by applying the public key algorithm $m = E_u(E_r^{-1}(m))$. Since the private key algorithm E_r^{-1} is only known by the gaming machine 120, the gaming server 110 can be particularly certain that the information m was sent by the gaming machine 120 because only the public key algorithm E_u is able to decrypt cipher-text c that has been encrypted using the private key algorithm E_r^{-1}.

As shown above, the digital signature is a variation of the asymmetric ~~session~~ key technique described above and can be fully implemented using asymmetric ~~session~~ keys. The digital signature provides an extra security feature that allows the receiving party to verify the sending party. This technique is particularly useful in the casino gaming system 100 when financial information, such as, credit card information, is being transmitted over the network bus 130.

It should be appreciated that the digital signature has been disclosed with reference to the gaming machine 120 and the gaming server 110 but should not be limited as such. The digital signature can be used by all devices connected to the network bus 130 and/or

the outside network 140. In addition, the encryption algorithm 180 used by the gaming server 110 to encrypt and transmit ~~session~~ keys 160 over the network bus 130 can comprise a digital signature.

B. Method For Using ~~Session~~ Keys

As shown in Fig. 2, the present invention includes a method for communicating information using a casino gaming system 100 having gaming machines 120-124 and a gaming server 110. The method includes establishing a first communication link (network bus 130 in Fig. 1) between the gaming machines 120-124 and the gaming server 110 (step 210). A second communication link (outside network 140 in Fig. 1) is established between the gaming server 110 and the remote computer 150 (step 220). It should be appreciated that the outside network 140 can comprise the Internet, a local access network (LAN) or a wide area network (WAN).

The gaming server 110 includes ~~session~~ keys 160. In one embodiment, the gaming server 110 includes a random number generator 170 that randomly generates the ~~session~~ keys 160 (step 230). The gaming server 110 can also include an encryption algorithm 180 that is used to encrypt the ~~session~~ keys 160 at the gaming server 110 (step 240). It should be appreciated that the ~~session~~ keys 160 and the encryption algorithm 180 can comprise symmetric ~~session~~ keys or asymmetric ~~session~~ keys that function as described herein above.

The ~~session~~ key 160 is transmitted from the gaming server 110 to, in one embodiment, a gaming machine 120 (step 250). It should be appreciated that the gaming server 110 can transmit the ~~session~~ key 160 to any other device connected to the network bus 130 or the outside network 140. The ~~session~~ key 160 is used by the gaming

server 110 to encrypt information sent from the gaming machine 120 (step 260). The encrypted information is transmitted over the first communication link (network bus 130) and/or the second communication link (outside network 140) (step 270). It should be appreciated that the encrypted information can be transmitted to another of the gaming machine 122-124, the gaming server 110 or the remote computer 150. Once the encrypted information is received, it is decrypted by the receiving device (such as, for example, gaming server 110) using a technique based on the type of ~~session~~ key 160 used as described herein above (step 280).

It should be appreciated that the method described with reference to gaming machine 120 and gaming server 110 is only for ease of description and should not be interpreted as being limited as such. It should be appreciated that the above described method can be used by any device connected to the network bus 130 and/or the outside network 140.

III. Certificate Authority

In general, as shown in Fig. 3, a certificate authority server 300 guarantees the identity of a device connected to the network bus 130 or connected to the outside network 140. The certificate authority 300 guarantees the identity by granting a unique public key 315 to each of the devices (as shown in Fig. 3, such as, gaming machines 120-124, gaming servers 330-332 and certificate servers 340-342) connected to the network bus 130. The certificate authority server 300 can also grant a unique public key to certain devices (such as remote computer 150) that are connected to the outside network 140. As noted above, there can be other certificate authority servers 340 and 342 connected to the network 130. All the certificate authority servers 300, 340 and 342 can be connected in a hierarchical configuration which is known in the art. In addition, there may be gaming servers 330-332 that do not have the ability to guarantee the identity of a device connected to the network bus 130. However, these gaming server 330-332 have the ability to perform other operations on the network bus 130, as described above with reference to Fig. 1.

A. Casino Gaming System using a Certificate Authority

As shown in Fig. 3, another embodiment of the casino gaming system 100 includes a certificate authority server 300 that is used for communicating information using asymmetric key pairs including a private key and a public key. In this embodiment, a network bus 130 interconnects the certificate authority 300 and the gaming machine 120-124. The network bus 130 can also be connected to other certificate authority servers 340-342 and gaming servers 330-332. The certificate authority server 300 includes a memory 310 that stores

public keys 315. The public keys 315 can also include a time stamp (not shown) that indicates a time period that the asymmetric key pair is used. The certificate authority server 300 also includes a random number generator 320 that is capable of generating the asymmetric key pairs of the present invention.

The certificate authority server 300 is also connected to an outside network 140 and a remote computer 150 is connected to the outside network 140. The outside network 140 can comprise the Internet, a local access network (LAN) or a wide area network (WAN). In another embodiment, it should be appreciated that the outside network 140 can connect to a gaming server 330-332 or another certificate authority server 340-342. The certificate authority server 300 can include other security mechanisms (not shown) to facilitate connection to the outside network 140, such as, for example, a firewall. The remote computer 150 can connect to the outside network 140 via, a hard wired connection, a wireless connection or a modem connection.

For ease of discussion, the certificate authority server 300 will be described with regard to transmissions to and from gaming machine 120 and gaming server 330. However, it should be appreciated that the certificate authority server 300 can transmit to any device on the network bus 130 and/or the outside network 140, and these devices can communicate using the same techniques as previously described with regard to the gaming machine 120 and the gaming server 110 (in Fig. 1).

In the present embodiment, when the gaming machine 120 desires to communicate with the gaming server 330, the gaming machine 120 requests a public key 315 from the certificate authority server 300. The certificate authority server 300 transmits a public key

315 to the gaming machine 120. The public key 315 is used by the gaming machine 120 to communicate with the gaming server 330 connected to the network bus 130. Prior to transmission of the pubic key 315, the certificate authority server 300 has verified the identity of the gaming server 330 and granted a unique asymmetric key pair to the gaming server 330. The verification is accomplished using various techniques known in the art. As a result of this verification, the certificate authority server 300 can guarantee the identity of the gaming server 330 and the validity of the public key 315 that is to be used by the gaming machine 120 to communicate with the gaming server 330.

In addition to transmitting the public key 315, the certificate authority server 300 signs the public key 315. The signing of the public key 315 uses an encryption algorithm that is similar to the symmetric and asymmetric ~~session~~ keys, such as, a digital signature, as described above. Once the gaming machine 120 receives the signed public key 315, the public key 315 is validated using, as described above, symmetric or asymmetric ~~session~~ key techniques. The gaming machine 120 uses the public key 315 to encrypt information and transmits that information over the network bus 130 to the gaming server 330.

As explained above, the gaming machine 120 can communicate with any other device connected to the network bus 130 and/or the outside network 140. However, these other devices must also be verified by the certificate authority server 300. As a result, the gaming machine 120 receives the appropriate public key 315 and transmits encrypted information to the appropriate device, such as, for example, other gaming machines 122-124, gaming severs 330-332, certificate authority servers 300, 340-342 and remote computer 150.

In a preferred embodiment, the certificate authority server 330 meets the X.509 (ISO/IEC 9594-8) standard.

IV. Remote Access

As shown in Fig. 4, another embodiment of the casino gaming system 100 includes switches 420, 422 and 424 that enable a remote player using a remote computer 150 to connect to and play a specific gaming machine 120-124 that is located in a casino.

A. Remote Access Casino Gaming System

In this embodiment, shown in Fig. 4, a network bus 130 interconnects a gaming server 110 and switches 420, 422 and 424. A certificate authority server 300 is also connected to the network bus 130. The certificate authority server 300 provides public keys 315 used for encrypting communications, as described above. The switches 420, 422 and 424 are connected to gaming machine 120, 122 and 124, respectively. In a preferred embodiment, the gaming machines 120, 122 and 124 are located in a casino. However, the physical location of the gaming machines 120, 122 and 124 should not be interpreted as limiting the present invention. The gaming server 110 is connected to an outside network 140 and a remote computer 150 is connected to the outside network 140.

In another embodiment, the outside network 140 can connect to the certificate authority server 300. The gaming server 110 can have various security features to facilitate connection to the outside network 140, such as, for example, a firewall. The outside network 140 can comprise the Internet, a local access network (LAN) or a wide area network (WAN). The remote computer 150 can be connected to

the outside network 140 via a hard wired connection, a wireless connection or a modem connection.

The present invention allows a remote player using a remote computer 150 to connect to and play a specific gaming machine 120-124 in a casino. For ease of description, the remote computer 150 will be described as connecting to gaming machine 120. However, it should be noted that the present invention encompasses the remote computer 150 connecting to any of the gaming machine 122-124 that are connected to the outside network 140. As such, the remote computer 150 connects to the outside network 140 which is connected to the gaming server 110. The remote computer 150 can be located in the casino, or the remote computer 150 can be located remotely from the casino, such as, but not limited to, a hotel connected to the casino.

To play the gaming machine 120, the remote computer 150 makes a request to the gaming server 110 to gain access to gaming machine 120. The request made by the remote computer 150 can include entering identification information that uniquely identifies the remote player of the remote computer 150. The identification information can comprise a password, credit card information, etc.

The gaming server 110 compares the identification information with a database. The database can include a listing of all passwords, a credit check of the credit card information or casino-specific credit information. If the identification information matches one of the entries in the database, the remote computer 150 is given access to the gaming machine 120 through switch 420.

It should be appreciated that, in another embodiment, the switch 420 disconnects the gaming machine 120 from access by the remote computer 150 when the gaming machine 120 is being used in

the casino. The disconnection of the gaming machine 120 can be initiated by a casino player in the casino. In this embodiment, if a casino player in the casino does not want a remote player connecting to the gaming machine 120, the casino player can activate switch 420 to prevent a remote player from accessing the gaming machine 120.

In addition, governmental regulation may require that only one person at a time can play a gaming machine 120 in the casino. In this case, the remote computer 150 receives a gaming machine unavailable signal when the gaming machine 120 is occupied and/or not idle, and the remote computer 150 is asked to choose another gaming machine 122-124. Conversely, if a remote computer 150 is accessing the gaming machine 120, a casino player cannot play the accessed gaming machine 120. In the casino, this disconnection is indicated by a light (not shown) or other indicators that verify that the gaming machine 120 is unavailable.

Once the remote computer 150 gains access to the gaming machine 120, the remote player can play the gaming machine 120. In one embodiment during play of the gaming machine 120, the remote player views a digital representation of the game being played on the gaming machine 120. The remote player can view and interact with the gaming machine 120 via other mechanisms that are known in the art.

The present invention should not be interpreted as being limited to the manner in which the remote player views and interacts with the play of the gaming machine 120. Furthermore, if the gaming machine 120 breaks down or malfunctions during play, the gaming machine 120 sends a signal to the remote computer 150 indicating that the gaming machine 120 is no longer available and the remote

player is asked to play another game and is credited any winnings from the gaming machine 120.

In addition, the communication between the remote computer 150 and the gaming machine 120 can be encrypted using symmetric or asymmetric ~~session~~ keys as described herein above. The gaming server 110 or the gaming machine 120 can document information with regard to the wagering during remote play of the gaming machine 120. Such information can include identification information about the remote player, amounts wagered, the time the remote player plays the gaming machine 120 and the location from which the remote player is playing the gaming machine 120.

B. Method Remotely Accessing Casino Gaming System

As shown in Fig. 5, a method is provided that allows a remote player to access and play a specific gaming machine 120-124 from a remote location. In this method, a request is received from an outside network 140 to access and play a gaming machine 120-124 (step 510). The request from the outside network 140 may be initiated by the input of identification information. The identification information can comprise a password, credit card information, etc. The gaming server 110 compares the identification information with a database.

The database can comprise a listing of all passwords, a credit check of the credit card information or casino-specific credit information. If the identification information matches one of the entries in the database, the remote computer 150 is given access to the gaming machine 120 through switch 420. It should be appreciated that, in another embodiment, the switch 420 disconnects

the gaming machine 120 from access by the remote computer 150 when the gaming machine 120 is being played in the casino. It should further be appreciated that the present invention is not limited to the type of request that is made by the remote computer 150 for access to the gaming machine 120.

Based on the request, a secured communication link is provided between the outside network 140 and the gaming machine 120-124 (step 530). In one embodiment, the secured communication link is only provided if the gaming machine 120-124 is idle and/or not being played by another player (step 520). In this embodiment, if the gaming machine 120 is not idle, a gaming machine unavailable message is provided to the outside network 140 (step 540). Additionally, the remote player can be asked to choose another of the gaming machines 122-124.

Once the outside network 140 accesses a gaming machine 120-124, information can be documented (step 550). The information can include identification information about the remote player, amounts wagered, the time the remote player plays the gaming machine 120 and the location from which the remote player is playing the gaming machine 120. When the remote player begins to play, the player views a digital representation of the gaming machine 120.

The foregoing discussion of the invention has been presented for purposes of illustration and description. Further, the description is not intended to limit the invention to the form disclosed herein. Consequently, variation and modification commensurate with the above teachings, within the skill and knowledge of the relevant art, are within the scope of the present invention.

The embodiment described herein and above is further intended to explain the best mode presently known of practicing the

invention and to enable others skilled in the art to utilize the invention as such, or in other embodiments, and with the various modifications required by their particular application or uses of the invention. It is intended that the appended claims be construed to include alternate embodiments to the extent permitted by the prior art.

WHAT IS CLAIMED IS:

1. A casino gaming system, comprising:

at least one gaming machine;

a gaming server including a plurality of ~~session~~ keys; and

a network bus interconnecting said at least one gaming machine and said gaming server, said network bus used to transmit information between said at least one gaming machine and said gaming server,

said gaming server transmitting at least one of said plurality of ~~session~~ keys over said network bus to said at least one gaming machine, said at least one gaming machine using said at least one of said plurality of ~~session~~ keys to encrypt said information and said at least one gaming machine transmitting said encrypted information over said network bus.

2. The casino gaming system, as claimed in Claim 1, wherein said plurality of ~~session~~ keys are symmetric keys.

3. The casino gaming system, as claimed in Claim 2, wherein said symmetric keys are session keys.

~~4~~3. The casino gaming system, as claimed in Claim 2, wherein said symmetric keys comprise Data Encryption Standard (DES) algorithms.

~~5~~4. The casino gaming system, as claimed in Claim 2, wherein said symmetric keys comprise triple Data Encryption Standard (triple-DES) algorithms.

65. The casino gaming system, as claimed in Claim 1, wherein said plurality of ~~session~~ keys comprise asymmetric key pairs.

7. The casino gaming system, as claimed in Claim 2, wherein said asymmetric keys are session keys.

86. The casino gaming system, as claimed in Claim 65, wherein said asymmetric key pairs comprise Rivest, Shamir, and Adleman (RSA) algorithms.

97. The casino gaming system, as claimed in Claim 1, wherein said gaming server is interconnected to an outside network.

108. The casino gaming system, as claimed in Claim 7, wherein said outside network is the Internet.

119. The casino gaming system, as claimed in Claim 1, wherein each of said plurality of ~~session~~ keys includes a time stamp, said time stamp indicating a period of time for which each of said plurality of ~~session~~ keys is used.

1210. The casino gaming system, as claimed in Claim 1, wherein said gaming server further comprises a random number generator that generates said plurality of ~~session~~ keys.

1311. The casino gaming system, as claimed in Claim 1, said gaming server further comprising:

an encryption algorithm, said gaming server using said encryption algorithm to encrypt said at least one of said plurality of ~~session~~ keys,

said gaming server transmitting said encrypted at least one of said plurality of ~~session~~ keys over said network bus to said at least one gaming machine.

1412. The casino gaming system, as claimed in Claim 1, wherein said encrypted information is transmitted over said network bus to another of said at least one gaming machines.

1513. The casino gaming system, as claimed in Claim 1, wherein said encrypted information is transmitted over said network bus to said gaming server.

1614. The casino gaming system, as claimed in Claim 1, further comprising:

an outside network connected to said gaming server; and

a remote computer connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote computer.

1715. A casino gaming system, comprising:

a plurality of gaming machines;

a gaming server comprising:

a plurality of ~~session~~ keys, each of said plurality of ~~session~~ keys including a time stamp, said time stamp indicating a period of time for which each of said plurality of ~~session~~ keys is used;

a random number generator that generates said plurality of ~~session~~ keys; and

an encryption algorithm;

a network bus interconnecting said plurality of gaming machines and said gaming server, said network bus used to transmit information between said plurality of gaming machines and said gaming server,

said gaming server using said encryption algorithm to encrypt at least one of said plurality of ~~session~~ keys,

said gaming server transmitting said at least one of said plurality of ~~session~~ keys over said network bus to at least one of said plurality of gaming machines where said ~~session~~ key is decrypted,

said at least one of said plurality of gaming machines using said at least one of said plurality of ~~session~~ keys to encrypt said information,

said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus.

18~~16~~. The casino gaming system, as claimed in Claim 17~~15~~, wherein said plurality of ~~session~~ keys are symmetric keys.

19. The casino gaming system, as claimed in Claim 18, wherein said symmetric keys are session keys.

20~~17~~. The casino gaming system, as claimed in Claim 17~~15~~, wherein said plurality of ~~session~~ keys comprise asymmetric key pairs.

21. The casino gaming system, as claimed in Claim 20, wherein said asymmetric keys are session keys.

2218. The casino gaming system, as claimed in Claim 1715, wherein said encrypted information is transmitted over said network bus to another of said plurality of gaming machines.

2319. The casino gaming system, as claimed in Claim 1715, wherein said encrypted information is transmitted over said network bus to said gaming server.

2420. The casino gaming system, as claimed in Claim 1715, further comprising:

an outside network connected to said gaming server; and

a remote computer connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote computer.

2521. A method for communicating information using a casino gaming system having at least one gaming machine and a gaming server, said method comprising the steps of:

establishing a first communication link between said at least one gaming machine and said gaming sever;

first transmitting at least one of a plurality of ~~session~~ keys stored at said gaming server over said first communication link from said gaming server to said at least one gaming machine;

encrypting information sent from said at least one gaming machine using said at least one of said plurality ~~session~~ keys;

second transmitting said encrypted information over said first communication link from said at least one gaming machine; and

decrypting said received encrypted information.

2622. The method, as claimed in Claim 2521, wherein said plurality of ~~session~~ keys include symmetric keys.

27. The method, as claimed in Claim 26, wherein said symmetric keys are session keys.

2823. The method, as claimed in Claim 2521, wherein said plurality of ~~session~~ keys include asymmetric key pairs.

29. The method, as claimed in Claim 28, wherein said symmetric keys are session keys.

3024. The method, as claimed in Claim 2521, further comprising the step of:

connecting said gaming server to an outside network.

3125. The method, as claimed in Claim 3024, wherein said outside network comprises the Internet.

3226. The method, as claimed in Claim 2521, further comprising the step of:

randomly generating said plurality of ~~session~~ keys at said gaming server.

3327. The method, as claimed in Claim 2521, further comprising the steps of:

encrypting each of said plurality of ~~session~~ keys transmitted from said gaming server to said at least one gaming machine.

3428. The method, as claimed in Claim 2521, wherein said step of second transmitting further comprises transmitting said encrypted information over said first communication link to another of said at least one gaming machine, and

wherein said step of decrypting further comprises decrypting said received encrypted information at said another of said at least one gaming machine.

3529. The method, as claimed in Claim 2521, wherein said step of transmitting further comprises second transmitting said encrypted information over said first communication link to said gaming server, and

wherein said step of decrypting further comprises decrypting said received encrypted information at said gaming server.

3630. The method, as claimed in Claim 2521, further comprising the step of:

establishing a second communication link between said gaming server and a remote computer.

3731. The method, as claimed in Claim 3630, wherein said step of transmitting further comprises transmitting said encrypted information over said first communication link and said second communication link to said remote computer, and

wherein said step of decrypting further comprises decrypting said received encrypted information at said remote computer.

3832. A casino gaming system for communicating information using asymmetric key pairs that includes a private key and a public key, said casino gaming system comprising:

a plurality of gaming machines;

a certificate authority server including a memory storing at least a plurality of said public keys of said asymmetric key pairs;

a network bus interconnecting said plurality of gaming machines and said certificate authority server,

said certificate authority server transmitting at least one of said plurality of public keys over said network bus to at least one of said plurality of gaming machines wherein said certificate authority server signs said at least one of said plurality of public keys transmitted over said network bus,

said at least one of said plurality of gaming machines using said at least one of said plurality of said public keys to encrypt information,

said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus.

3933. The casino gaming system, as claimed in Claim 3832, wherein each of said plurality of gaming machines validates said at least one of said signed plurality of public keys received from said network bus.

4034. The casino gaming system, as claimed in Claim 3832, wherein said certificate authority server is connected to an outside network.

4135. The casino gaming system, as claimed in Claim 4034, wherein said outside network comprises the Internet.

4236. The casino gaming system, as claimed in Claim 3832, wherein said encrypted information is transmitted over said network bus to another of said at least one gaming machines.

4337. The casino gaming system, as claimed in Claim 3832, wherein said encrypted information is transmitted over said network bus to said gaming server.

4438. The casino gaming system, as claimed in Claim 3832, further comprising:

an outside network connected to said gaming server; and

a remote computer connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote computer.

4539. The casino gaming system, as claimed in Claim 3832, wherein said network bus is connected to at least one gaming server,

said certificate authority server transmitting at least one of said plurality of said public keys to said at least one gaming server,

said gaming server encrypts information using said at least one of said plurality of said public keys,

said gaming server transmits said encrypted information over said network bus.

4640. The casino gaming system, as claimed in Claim 3832, wherein said certificate authority server comprises a random number generator for generating said plurality of said asymmetric key pairs.

4741. The casino gaming system, as claimed in Claim 3832, wherein each of said asymmetric key pairs includes a time stamp, said time stamp indicating a period of time for which said asymmetric key pairs are used.

4842. The casino gaming system, as claimed in Claim 3832, wherein said network bus is connected to a plurality of other certificate authority servers, said certificate authority server transmitting at least one of said plurality of said public keys to said plurality of other certificate authority servers wherein said plurality of other certificate authority servers encrypts information using said at least one of said plurality of said public keys and transmits said encrypted information over said network bus.

4943. A casino gaming system connected to at least one outside computer via an outside network, said casino gaming system comprising:

a gaming server;

a plurality of gaming machines located in a casino;

a plurality of access switches, each one of said plurality of access switches individually connected to a different one of said plurality of gaming machines; and

a network bus connected to said gaming server and each of said plurality of access switches;

said outside network connected to said gaming server,

one of said plurality of access switches connecting one of said plurality of gaming machines and said outside computer over said outside network when said one of said plurality of gaming machines is idle, so as to enable a remote player of said outside computer to play said one of said plurality of gaming machines.

5044. The casino gaming system, as claimed in Claim 4943, wherein said outside network comprises the Internet.

5145. The casino gaming system, as claimed in Claim 4943, further comprising:

a certificate authority server connected to said network bus, said certificate authority server including a plurality of public keys of a plurality of asymmetric key pairs.

5246. The casino gaming system, as claimed in Claim 5145, wherein said outside computer acquires one of said plurality of public keys from said certificate authority server via said outside network and said network bus, said outside computer using said one of said plurality of public keys to encrypt information transmitted to said one of said plurality of gaming machines over said outside network and said network bus.

5347. The casino gaming system, as claimed in Claim 4943, wherein information communicated between said outside computer and said one of said plurality of gaming machines over said outside network and said network bus is encrypted using asymmetric key pairs.

5448. The casino gaming system, as claimed in Claim 4943, wherein information communicated between said outside computer and said one of said plurality of gaming machines over said outside network and said network bus is encrypted using symmetric keys.

5549. A casino gaming system connected to at least one outside computer via an outside network, said casino gaming system comprising:

a gaming server;

a plurality of gaming machines;

a plurality of access switches, each one of said plurality of access switches individually connected to a different one of said plurality of gaming machines; and

a network bus connected to said gaming server and each of said plurality of access switches;

said outside network connected to said gaming server,

one of said plurality of access switches connecting one of said plurality of gaming machines and said outside computer over said outside network, so as to enable a remote player of said outside computer to play said one of said plurality of gaming machines.

5650. The casino gaming system, as claimed in Claim 5549, wherein said gaming machines are located in a casino.

5751. The casino gaming system, as claimed in Claim 5549 wherein said one of said plurality of access switches provides said communication link when said one of said plurality of gaming machines is idle.

5852. A method for communicating with a plurality of gaming machines in a casino, said plurality of gaming machines connected to a gaming server, said method comprising the steps of:

receiving a request from an outside network for an identified one of said plurality of gaming machines, said request initiated by a remote player;

providing a secured communication link between said outside network and said identified one of said plurality of gaming machines when said identified one of said plurality of gaming machines is idle, so as to enable the remote player to play a casino game at said identified one of said plurality of gaming machines; and

delivering to said outside network a gaming machine unavailable message when said identified one of said plurality of gaming machines is in use.

5953. The method, as claimed in Claim 5852, wherein said step of receiving a request further comprising the steps of:

entering player identification information; and

providing said entered player identification information to a database.

6054. The method, as claimed in Claim 5953, wherein said step of providing said entered player identification information further comprises the steps of:

comparing said entered player identification information to said database; and

providing said secured communication link between said outside network and said identified one of said plurality of gaming

machines if said entered identification information matches an entry in said database.

6255. The method, as claimed in Claim 5953, wherein said entered player identification information is credit card information.

6356. The method, as claimed in Claim 5852, further comprising the steps of:

documenting information about the remote player.

6457. The method, as claimed in Claim 6356, wherein said documented information comprises information about the remote player.

6558. The method, as claimed in Claim 6356, wherein said documented information comprises a time for which the remote player plays said one of said plurality of gaming machines.

6659. The method, as claimed in Claim 6356, wherein said documented information comprises a location from which the remote player is playing.

6760. The method, as claimed in Claim 6356, wherein said documented information comprises an amount the remote player has wagered.

6861. The method, as claimed in Claim 5852, wherein said outside network comprises the Internet.

6962. A method for communicating with a plurality of gaming machines, said plurality of gaming machines connected to a gaming server, said method comprising the steps of:

receiving a request from an outside network for an identified one of said plurality of gaming machines, said request initiated by a remote player;

providing a secured communication link between said outside network and said identified one of said plurality of gaming machines, so as to enable the remote player to play a casino game at said identified one of said plurality of gaming machines; and

delivering to said outside network a gaming machine unavailable message when said identified one of said plurality of gaming machines is in use.

7063. The method, as claimed in Claim 6962, wherein said plurality of gaming machines are located in a casino.

7164. The method as claimed in Claim 6962, wherein said step of providing a secured communication link provides said secured communication link when said identified one of said plurality of gaming machines is idle.

CRYPTOGRAPHY AND CERTIFICATE AUTHORITIES IN GAMING MACHINES

ABSTRACT

The casino gaming system includes gaming machines and a gaming server having ~~session~~ keys. A network bus interconnects the gaming machines and the gaming server. The network bus provides a communication link to transmit information between the gaming machine and the gaming server. The gaming server transmits ~~session~~ keys over the network bus to the gaming machines. The gaming machines use the ~~session~~ keys to encrypt information, and the gaming machines transmit the encrypted information over the network bus and/or an outside network connected to the gaming server.

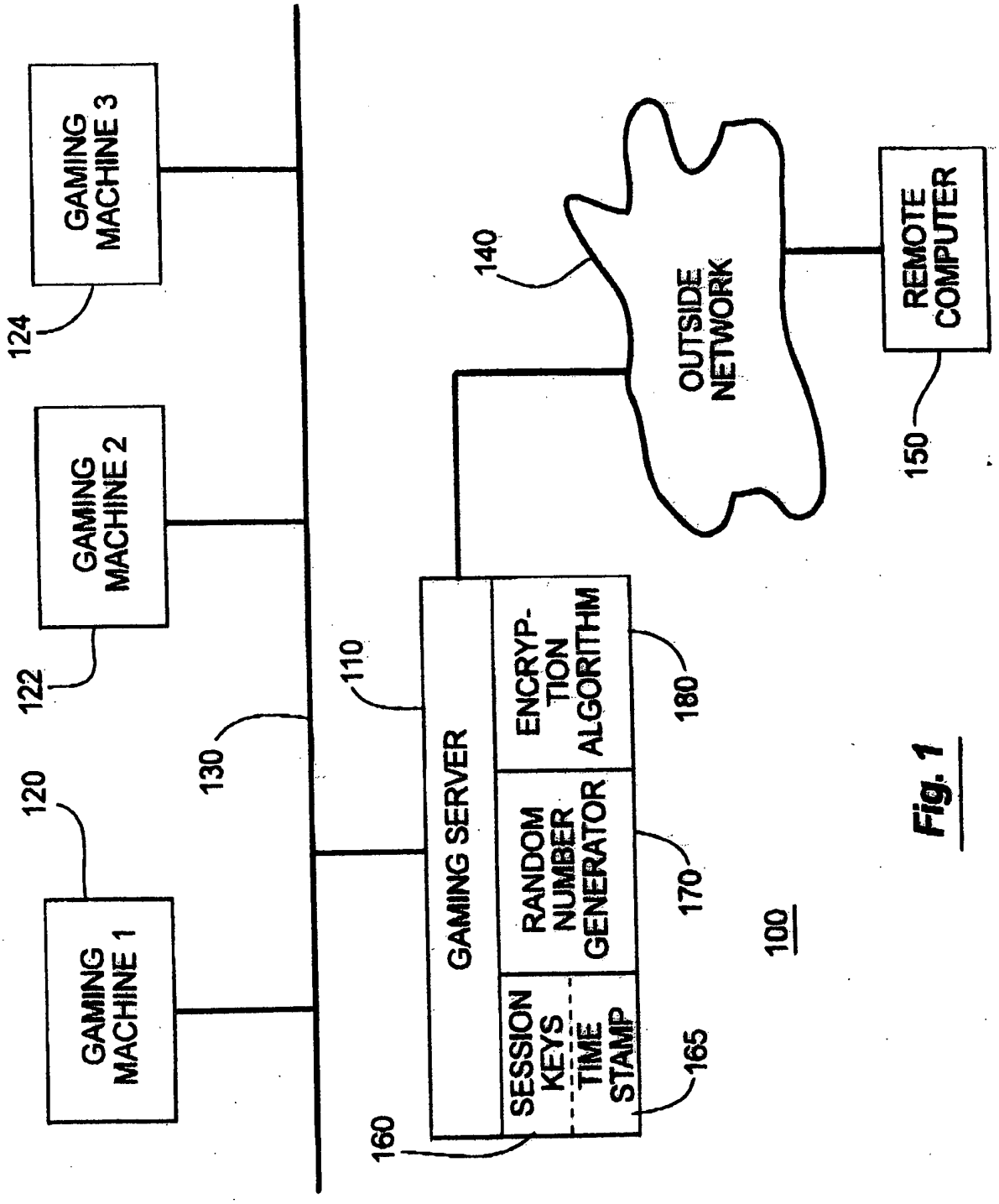
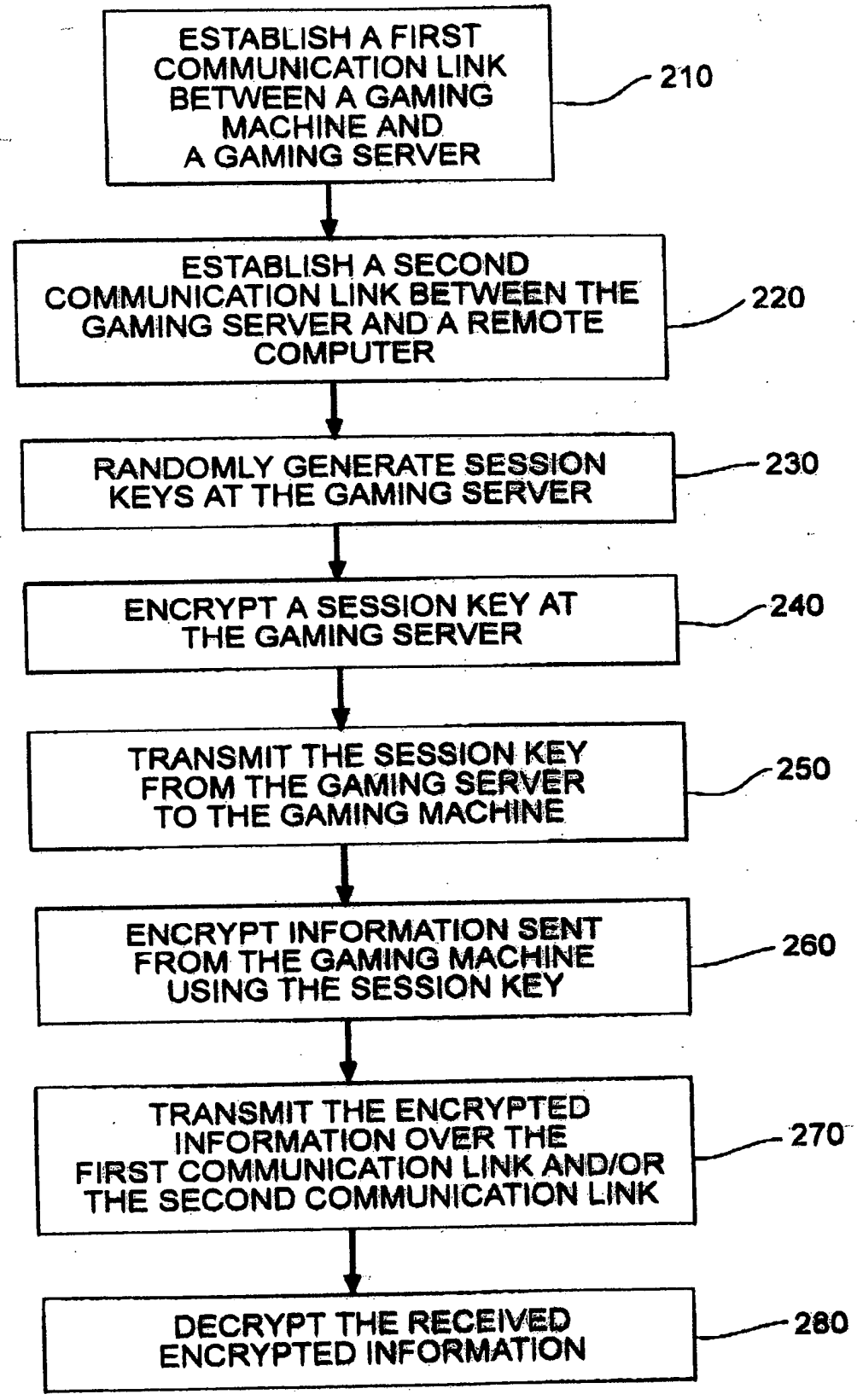

GAMING MACHINE 3
124
GAMING MACHINE 2
122
GAMING MACHINE 1
120
130
110
GAMING SERVER
ENCRYP-TION ALGORITHM
180
RANDOM NUMBER GENERATOR
170
SESSION KEYS
TIME STAMP
165
160
140
OUTSIDE NETWORK
REMOTE COMPUTER
150
100

Fig. 1

Fig. 2


ESTABLISH A FIRST COMMUNICATION LINK BETWEEN A GAMING MACHINE AND A GAMING SERVER
210
ESTABLISH A SECOND COMMUNICATION LINK BETWEEN THE GAMING SERVER AND A REMOTE COMPUTER
220
RANDOMLY GENERATE SESSION KEYS AT THE GAMING SERVER
230
ENCRYPT A SESSION KEY AT THE GAMING SERVER
240
TRANSMIT THE SESSION KEY FROM THE GAMING SERVER TO THE GAMING MACHINE
250
ENCRYPT INFORMATION SENT FROM THE GAMING MACHINE USING THE SESSION KEY
260
TRANSMIT THE ENCRYPTED INFORMATION OVER THE FIRST COMMUNICATION LINK AND/OR THE SECOND COMMUNICATION LINK
270
DECRYPT THE RECEIVED ENCRYPTED INFORMATION
280

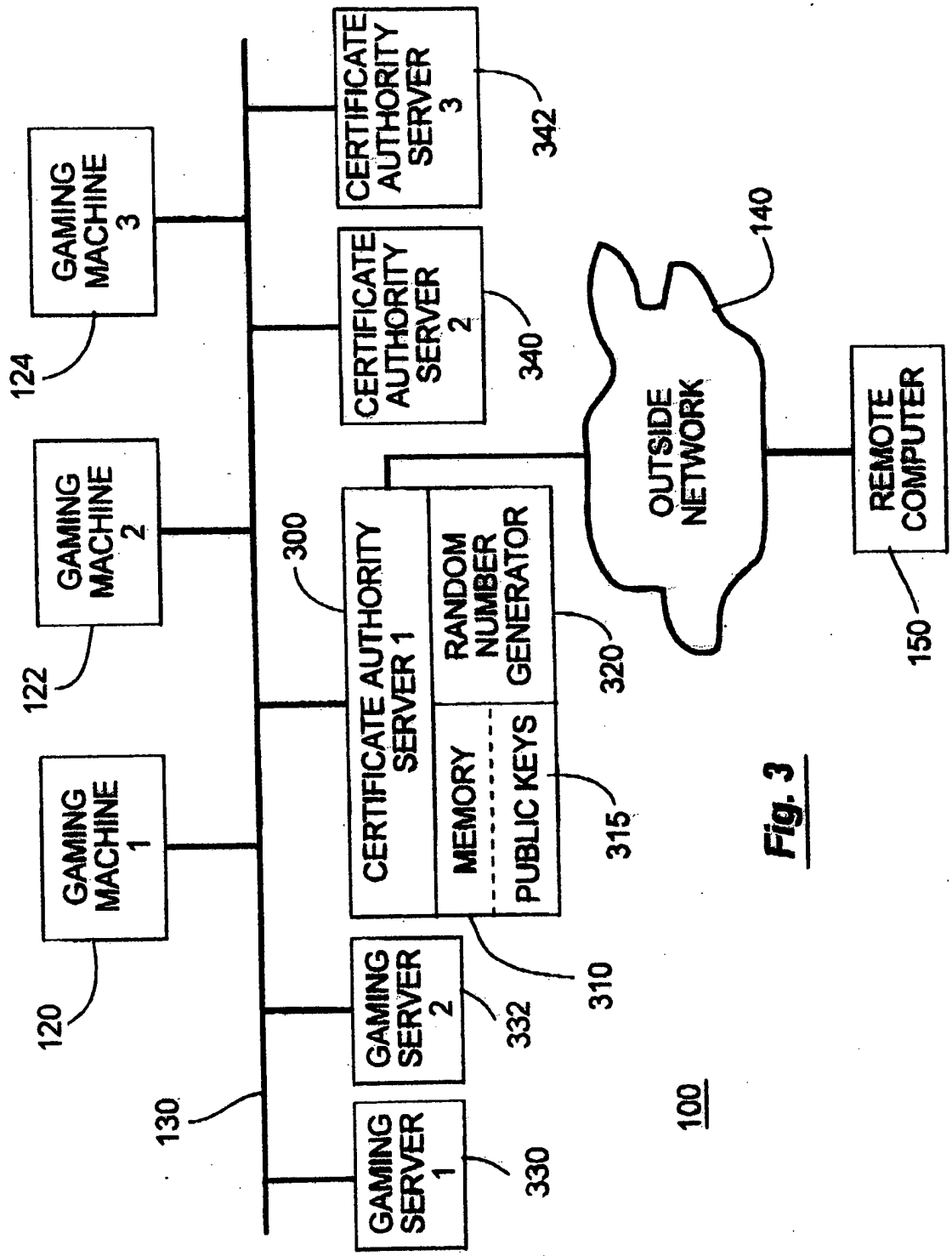

GAMING MACHINE 3
124
GAMING MACHINE 2
122
GAMING MACHINE 1
120
130
GAMING SERVER 1
330
GAMING SERVER 2
332
CERTIFICATE AUTHORITY SERVER 1
300
MEMORY
PUBLIC KEYS
310
315
RANDOM NUMBER GENERATOR
320
CERTIFICATE AUTHORITY SERVER 2
340
CERTIFICATE AUTHORITY SERVER 3
342
OUTSIDE NETWORK
140
REMOTE COMPUTER
150
100

Fig. 3

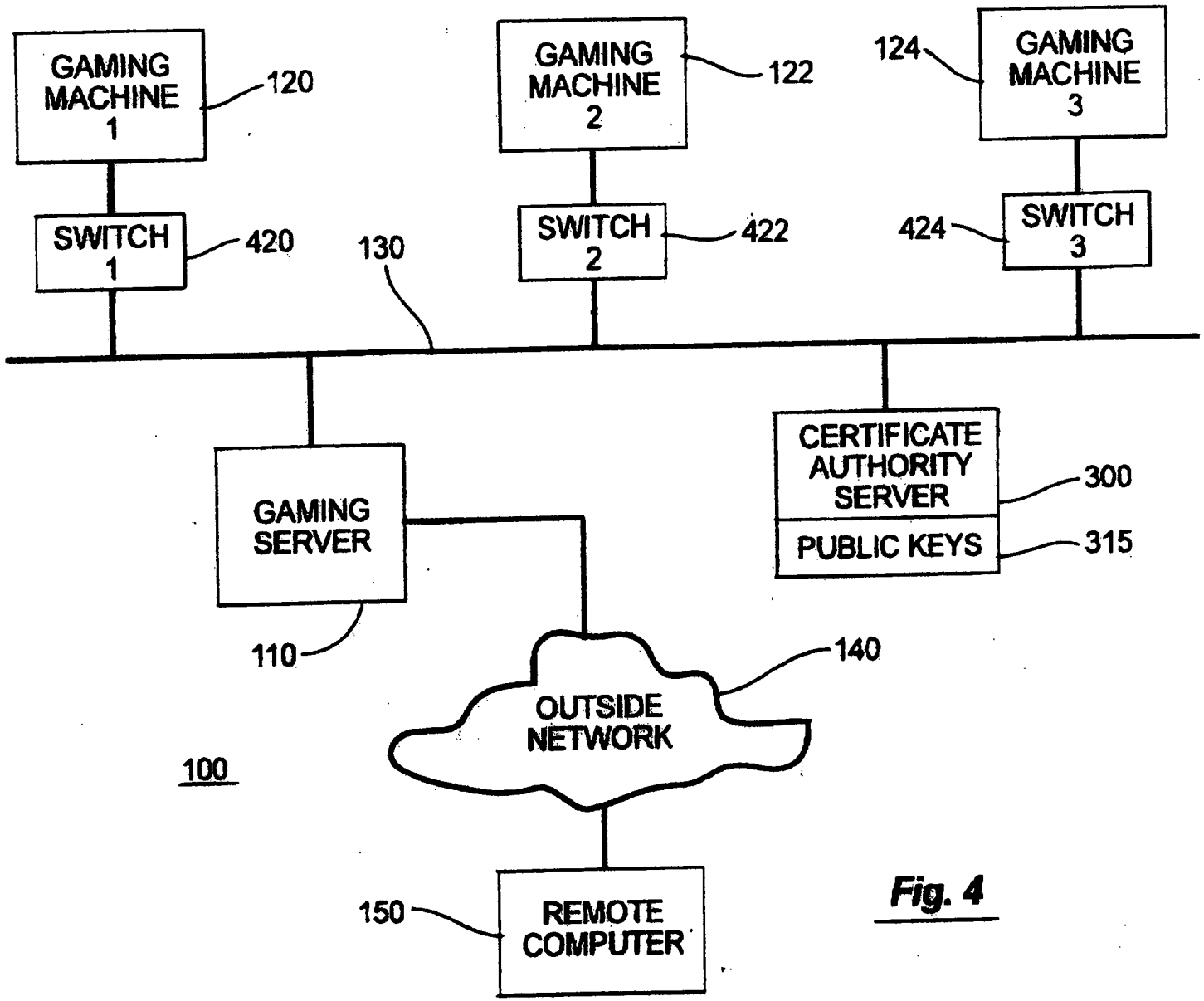

GAMING MACHINE 1
120
GAMING MACHINE 2
122
124
GAMING MACHINE 3
SWITCH 1
420
130
SWITCH 2
422
424
SWITCH 3
CERTIFICATE AUTHORITY SERVER
300
PUBLIC KEYS
315
GAMING SERVER
110
140
OUTSIDE NETWORK
100
150
REMOTE COMPUTER

Fig. 4

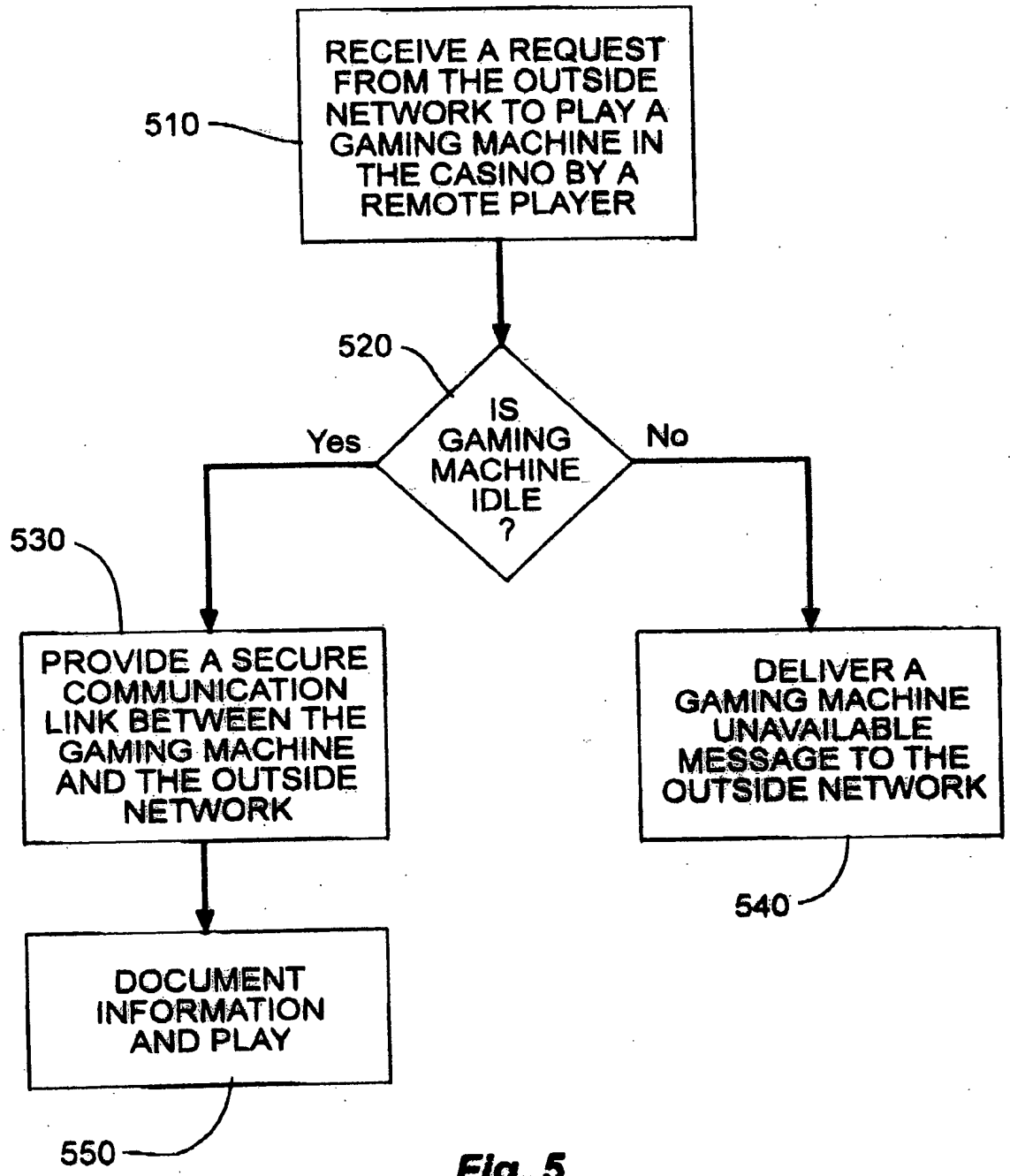

RECEIVE A REQUEST FROM THE OUTSIDE NETWORK TO PLAY A GAMING MACHINE IN THE CASINO BY A REMOTE PLAYER
510
520
IS GAMING MACHINE IDLE ?
Yes
No
530
PROVIDE A SECURE COMMUNICATION LINK BETWEEN THE GAMING MACHINE AND THE OUTSIDE NETWORK
DELIVER A GAMING MACHINE UNAVAILABLE MESSAGE TO THE OUTSIDE NETWORK
540
DOCUMENT INFORMATION AND PLAY
550

Fig. 5